Q&A /// INTERVIEW WITH AN INDUSTRY INSIDER

JOE COLEMAN /// CYBER SECURITY OFFICER /// BLUESTREAK CONSULTING

"The future of your company depends on this certification; start now, because the clock is officially running; don't wait until it's too late."

What Is CMMC 2.0?

CMMC stands for Cybersecurity Maturity Model Certification. CMMC 2.0 is a contractual requirement for any non-federal organization or system that is part of the Defense Industrial Base (DIB) or falls anywhere within the DoD supply chain and who handles Controlled Unclassified Information (CUI) in any way. The CMMC 2.0 requirements are based on NIST SP 800-171 Rev.2 requirements.

There are 3 levels to CMMC 2.0:

›› **Level 1 is Foundational.** This is appropriate for companies that do handle Federal Contract Information (FCI) but do not handle CUI.

›› **Level 2 is Advanced.** This level is for any company that stores, processes, or transmits CUI, whether it is in electronic or paper form. Basically, the same as NIST SP 800-171 requirements.

›› **Level 3 is Expert.** This level includes highly advanced cybersecurity practices.

The majority of business will need to be at Level 2.

Why is CMMC 2.0 so important for heat treaters and other businesses?

When the deadline approaches for companies to be fully compliant, which is coming quickly. The DoD and its contractors will be requiring full compliance to NIST SP 800-171 requirements prior to any company receiving a contract or order or at least being able to show that your implementation is in process with a date of full compliance. You will first do a security assessment on your systems and facilities.

From the results of the assessment, you will need to generate a Plan Of Action with Milestones (POA&M) listing all noncompliance. NIST SP 800-171 consists of 110 security controls corresponding to 14 control families ranging from 3.1 Access Control to 3.14 System & Information Integrity.

Within the 110 controls, there are 320 control/assessment objectives, all of which need to be met. CMMC 2.0 is different. You will need a perfect score of 110 in order to be certified, and this certification process will be done by a CMMC Third Part Assessment Organization (C3PAO).

What should heat treaters be doing now?

Because CMMC 2.0's requirements are based on NIST SP 800-171 Rev. 2 security requirements, your company should have already started with this implementation. NIST SP 800-171 compliance can be done through self-attestation. You will be scored on each of the 110 controls on a weighted scale of 1, 3, or 5 points. A perfect score is 110, whereas the worst score can be as low as minus-203. You'll need to submit that score to the Supplier Performance Risk System (SPRS) to make it official.

How do heat treaters become CMMC 2.0 certified?

They'll need to become NIST SP 800-171 fully compliant and get to the point of CMMC audit ready. Once you are ready for your final certification audit, you will need to schedule this audit with a C3PAO. There will be a huge backlog because there are only 49 certified C3PAOs to perform these audits, and there will be over 74,000 businesses that will need to be CMMC 2.0 Level 2 certified. Overall, CMMC will affect nearly 300,000 businesses nationwide.

How long does it take to become CMMC 2.0 Certified?

To become certified, it can take anywhere between 12 to 24 months based on your current cybersecurity status and infrastructure. CMMC requirements include controls from access control to incident response, to physical protection. These requirements are very detailed, and all need to be met to become certified.

What is the deadline to become CMMC 2.0 Certified?

When CMMC 1.0 first rolled out in 2020, it was a mess. Originally everyone needed to be certified by September of 2020. Then we had the pandemic, and everything changed, and that did not happen. Then, in 2021, the DoD released CMMC 2.0, which simplified CMMC 1.0. On December 26, 2023, they released CMMC 2.0 for a comment period. Once this period is over, it is expected to be fully released by the end of 2024 or Q1 2025. Meanwhile, this is a rolled-out approach, meaning that by the end of 2027 or the first of 2028, CMMC 2.0 will be a full-contract requirement.

What happens if a company ignores or fails to become CMMC 2.0 certified?

If a company fails to become NIST SP 800-171 compliant and CMMC 2.0 certified, that business risks losing current DoD contracts/business and will not be eligible to receive new DoD contracts/business. The future of your company depends on this certification. Start now, because the clock is officially running. Don't wait until it's too late. This can be a long and difficult process.

To ensure this is done correctly and efficiently, don't try this on your own. You should seek the help of a certified CMMC RPA (Registered Practitioner Advanced) to get you through the implementation process.

MORE INFO go-bluestreak.com